Topics:

awareness [2], security training [3], security awareness [4], training [5], employee [6], third-party [7], contractor [8], annual training [9], unescorted [10], physical access [11], public access [12]

SS-08-012.02 Security Education and Awareness

Issue Date: 3/31/2008

Revision Effective Date: 12/15/2014

PURPOSE

One of the goals of the State?s Information Security Program is to increase the awareness of the workforce through a security awareness program. Organizations cannot protect the integrity, confidentiality, and availability of information in today?s highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them. NIST Special Publication 800-50, developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, states ?the people factor - not technology - is key to providing an adequate and appropriate level of security?. If people are the key, but are also a weak link, ?a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.?

SCOPE, AUTHORITY, ENFORCEMENT, EXCEPTIONS

Enterprise Information Security Charter (PS-08-005) [13]

STANDARD

All state agencies shall provide information security awareness training to their employees and engagement contractors who have unescorted logical or physical access to state facilities and/or information resources not designated as public access resources.

The training shall be conducted annually, attendance shall be mandatory, and training completion shall be documented in personnel and contractor training records.

Awareness training shall provide practical and simple guidance pertaining to employee and contractor roles and responsibilities for protecting the state?s information assets, incident reporting and contingency preparedness. It shall provide updates to and reinforce security policies and procedures and highlight overall awareness. The training must include information regarding the state?s and the agency?s information security policies and standards, and where to find them. It must also include any training required by applicable information owners.

Additional role-based security training shall be provided to applicable information owners, IT specialists, developers, the security management organization, and others that have unique or specific information security responsibilities.

If engagement contractors provide training to their employees, agencies shall define the requirements for and review contractor training materials to ensure that all state and agency required training content are included and appropriate (such as state and agency policies and procedures, HIPAA, CJIS, FTI, etc). Agencies shall review training records of contractors to ensure that all engaged employees obtain the training annually.